

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000181803 A**

(43) Date of publication of application: **30 . 06 . 00**

(51) Int. Cl.

G06F 12/14
G09C 1/00
H04L 9/08

(21) Application number: **10360345**

(22) Date of filing: **18 . 12 . 98**

(71) Applicant: **FUJITSU LTD**

(72) Inventor: **KURODA YASUTSUGU**
KAMATA JUN
IWASE SHIYOUKO
NODA TOSHITATSU
ONO KOSHIO

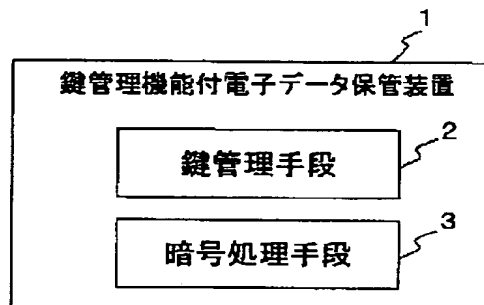
(54) **ELECTRONIC DATA KEEPING DEVICE WITH
KEY MANAGEMENT FUNCTION AND METHOD
THEREFOR**

(57) Abstract:

PROBLEM TO BE SOLVED: To realize key management corresponding to environment and also to secure safety in electronic data by executing communication through the use of a common key being adaptable to both local and global environments.

SOLUTION: An electronic data keeping device is provided with a means 2 for managing an individual key being intrinsic to a self-keeping device and also the common key shared with another keeping device and with a means 3 for executing a ciphering processing through the use of the individual key in electronic data which is kept in the self device and for executing the ciphering processing or inspecting data through the use of the common key in electronic data which is exchanged with another device.

COPYRIGHT: (C)2000,JPO



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-181803

(43)Date of publication of application : 30.06.2000

(51)Int. Cl.

G06F 12/14

G09C 1/00

H04L 9/08

(21)Application number : 10-360345

(71)Applicant : FUJITSU LTD

(22)Date of filing : 18.12.1998

(72)Inventor : KURODA YASUTSUGU

KAMATA JUN

IWASE SHIYOUKO

NODA TOSHITATSU

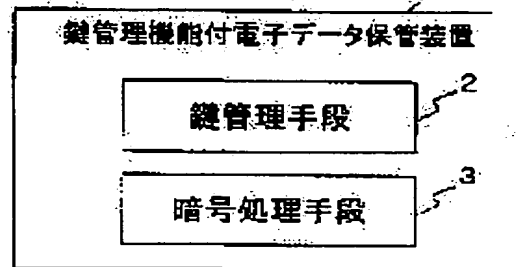
ONO KOSHIO

(54) ELECTRONIC DATA KEEPING DEVICE WITH KEY MANAGEMENT FUNCTION AND METHOD THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To realize key management corresponding to environment and also to secure safety in electronic data by executing communication through the use of a common key being adaptable to both local and global environments.

SOLUTION: An electronic data keeping device is provided with a means 2 for managing an individual key being intrinsic to a self-keeping device and also the common key shared with another keeping device and with a means 3 for executing a ciphering processing through the use of the individual key in electronic data which is kept in the self device and for executing the ciphering processing or inspecting data through the use of the common key in electronic data which is exchanged with another device.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-181803

(P 2 0 0 0 - 1 8 1 8 0 3 A)

(43) 公開日 平成12年6月30日(2000.6.30)

(51) Int. Cl. ⁷	識別記号	F I	テ-マ-ト (参考)	
G06F 12/14	320	G06F 12/14	320	B 5B017
G09C 1/00	660	G09C 1/00	660	E 5J104
			660	F 9A001
H04L 9/08		H04L 9/00	601	B
			601	E
審査請求 未請求 請求項の数21 O L (全23頁)				

(21) 出願番号 特願平10-360345

(22) 出願日 平成10年12月18日(1998.12.18)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 黒田 康嗣

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 蒲田 順

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 100074099

弁理士 大菅 義之 (外1名)

最終頁に続く

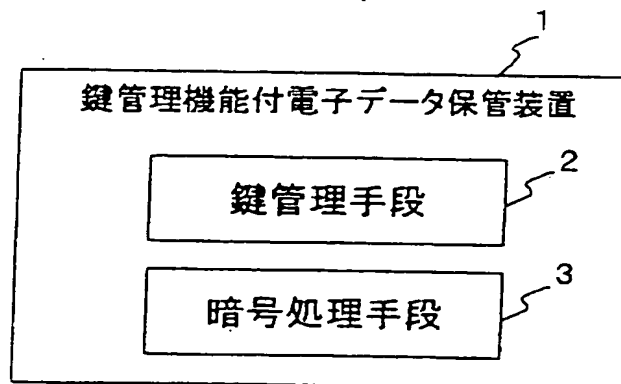
(54) 【発明の名称】 鍵管理機能付電子データ保管装置および電子データ保管方法

(57) 【要約】

【課題】 ローカルな環境とグローバルな環境にそれぞれ適合した共通鍵を用いて通信を行って環境に合った鍵管理を実現するとともに、電子データの安全性を確保する。

【解決手段】 自保管装置に固有の個別鍵と、他の保管装置との間で共通の共通鍵とを管理する手段2と、自装置内に保管する電子データに対しては個別鍵を用いて暗号処理を行い、他装置との間で送信、または受信する電子データに対しては共通鍵を用いて暗号処理、またはデータ検証を行う手段3とを備える。

本発明の原理構成ブロック図



【特許請求の範囲】

【請求項 1】 電子データを保管する電子データ保管装置において、

自電子データ保管装置に固有の個別鍵と、他の電子データ保管装置との間で共通の共通鍵とを管理する鍵管理手段と、

自電子データ保管装置内に保管する電子データに対しては前記個別鍵を用いて暗号処理を行い、他電子データ保管装置との間で送信、または受信する電子データに対しては、前記共通鍵を用いて暗号処理、またはデータ検証を行う暗号処理手段とを備えることを特徴とする鍵管理機能付電子データ保管装置。

【請求項 2】 前記鍵管理手段が、前記共通鍵として複数の電子データ保管装置によって構成される 1 つのグループ内で共通のグループ鍵を管理することを特徴とする請求項 1 記載の鍵管理機能付電子データ保管装置。

【請求項 3】 前記 1 つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて該 1 つのグループ内の個々の電子データ保管装置の個別鍵を生成し、

該生成された個別鍵が該 1 つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項 2 記載の鍵管理機能付電子データ保管装置。

【請求項 4】 前記 1 つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて前記 1 つのグループ内で共通のグループ鍵を生成し、

該生成されたグループ鍵が該 1 つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項 2 記載の鍵管理機能付電子データ保管装置。

【請求項 5】 前記 1 つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、前記個別鍵として該主となる電子データ保管装置の使用開始前にあらかじめ割り当てられている鍵と、新たに外部から指定される鍵とを関連づけて前記 1 つのグループ内で共通のグループ鍵を生成し、

該生成されたグループ鍵が該 1 つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項 2 記載の鍵管理機能付電子データ保管装置。

【請求項 6】 前記 1 つのグループ内に主となる電子データ保管装置が存在すると共に、該複数のグループ内の該主となる電子データ保管装置のそれぞれを管理するグループ管理用電子データ保管装置が存在し、

該グループ管理用電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて該主となる電子データ保管装置のそれぞれの個別鍵を生成し、

該生成された個別鍵が該主となる電子データ保管装置の

それぞれに配布されることを特徴とする請求項 2 記載の鍵管理機能付電子データ保管装置。

【請求項 7】 前記鍵管理手段が前記共通鍵として、前記グループ鍵に加えて、自電子データ保管装置が属するグループと異なるグループに属する電子データ保管装置との間での電子データの送受信に用いられる公開鍵を管理することを特徴とする請求項 2 記載の鍵管理機能付電子データ保管装置。

【請求項 8】 前記個別鍵が前記電子データ保管装置の使用開始前にあらかじめ各電子データ保管装置に割り当てられていることを特徴とする請求項 1 記載の鍵管理機能付電子データ保管装置。

【請求項 9】 前記暗号処理手段が、自電子データ保管装置の使用開始前にあらかじめ設定されている鍵と、外部から新たに指定される鍵とを関連づけて前記個別鍵を生成し、

前記鍵管理手段が該生成された個別鍵を管理することを特徴とする請求項 1 記載の鍵管理機能付電子データ保管装置。

【請求項 10】 前記鍵管理手段が、前記個別鍵と共通鍵とに加えて、全ての電子データ保管装置に共通のマスター鍵を管理することを特徴とする請求項 1 記載の鍵管理機能付電子データ保管装置。

【請求項 11】 前記暗号処理手段が、前記マスター鍵を用いて自電子データ保管装置を識別する情報を暗号化して、前記個別鍵を生成し、

前記鍵管理手段が該生成された個別鍵を管理することを特徴とする請求項 10 記載の鍵管理機能付電子データ保管装置。

【請求項 12】 複数の電子データ保管装置によって構成される 1 つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、前記生成された個別鍵を用いて前記 1 つのグループを識別する情報を暗号化して前記共通鍵としてのグループ鍵を生成し、

該生成されたグループ鍵が該 1 つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項 11 記載の鍵管理機能付電子データ保管装置。

【請求項 13】 それぞれ複数の電子データ保管装置によって構成されるグループを 1 つの階層とする電子データ保管装置の階層構造が構成され、

前記鍵管理手段が、自装置が属するグループの階層に応じたグループ鍵を前記共通鍵として管理することを特徴とする請求項 1 記載の鍵管理機能付電子データ保管装置。

【請求項 14】 前記電子データ保管装置の階層構造において、上位側の階層のグループ内に直近下位の階層のグループの電子データ保管装置を管理する管理用電子データ保管装置が存在し、

該管理用電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて該下位階層に対応するグループ鍵を生成し、

該生成されたグループ鍵が該直近下位の階層のグループの電子データ保管装置に配布されることを特徴とする請求項 13 記載の鍵管理機能付電子データ保管装置。

【請求項 15】 それぞれ複数の電子データ保管装置によって構成されるグループを 1 つの階層とする階層構造内の電子データ保管装置における電子データ保管方法であって、

該階層構造の 1 つの階層内の送信側電子データ保管装置が、自装置内に保管され、自装置に固有の個別鍵を用いて暗号処理されているデータを、該 1 つの階層に対応する上位グループ鍵によって暗号処理し直して、該階層構造で直近下位の階層の電子データ保管装置を管理する下位グループ管理用電子データ保管装置に送信し、

該下位グループ管理用電子データ保管装置が前記上位グループ鍵を用いて受信したデータを検証し、

該検証の結果、電子データが正しければ前記直近下位の階層に対応する下位グループ鍵によって該電子データを暗号処理し直して該直近下位階層内の受信側電子データ保管装置に送信し、

該受信側電子データ保管装置が該下位グループ鍵を用いて受信データを検証し、

該検証の結果、電子データが正しければ、自装置に固有の個別鍵を用いて受信データを暗号処理し直して保管することを特徴とする電子データ保管方法。

【請求項 16】 それぞれ複数の電子データ保管装置によって構成されるグループを 1 つの階層とする階層構造内の電子データ保管装置における電子データ保管方法であって、

該階層構造の 1 つの階層内の送信側電子データ保管装置が、自装置内に保管され、自装置に固有の個別鍵を用いて暗号処理されているデータを、該 1 つの階層に対応する下位グループ鍵によって暗号処理し直して、該 1 つの階層の電子データ保管装置を管理する下位グループ管理用電子データ保管装置に送信し、

該下位グループ管理用電子データ保管装置が前記下位グループ鍵を用いて受信したデータを検証し、

該検証の結果、電子データが正しければ前記 1 つの階層の直近上位の階層に対応する上位グループ鍵によって該電子データを暗号処理し直して該直近上位階層内の受信側電子データ保管装置に送信し、

該受信側電子データ保管装置が該上位グループ鍵を用いて受信データを検証し、

該検証の結果、電子データが正しければ、自装置に固有の個別鍵を用いて受信データを暗号処理し直して保管することを特徴とする電子データ保管方法。

【請求項 17】 電子データを保管する電子データ保管装置における電子データ保管方法であって、

他の電子データ保管装置との間で共通の共通鍵を用いて電子データの通信を行い、

自電子データ保管装置に保管すべきデータに対しては自電子データ保管装置に固有の個別鍵を用いて暗号処理を行うことを特徴とする電子データ保管方法。

【請求項 18】 前記電子データ保管装置が、前記共通鍵として複数の電子データ保管装置によって構成される 1 つのグループ内で共通のグループ鍵を保存し、

送信側の電子データ保管装置が、自電子データ保管装置内に保管され、前記個別鍵を用いて暗号処理されている電子データを該グループ鍵によって暗号処理し直して、該電子データを送信し、

受信側の電子データ保管装置が受信した電子データを該グループ鍵を用いて検証し、

検証の結果、電子データが正しければ、該電子データを前記個別鍵を用いて暗号処理し直して保管することを特徴とする請求項 17 記載の電子データ保管方法。

【請求項 19】 前記電子データ保管装置が前記共通鍵として、複数の電子データ保管装置によって構成され、自電子データ保管装置が属する 1 つのグループと異なる他のグループに属する電子データ保管装置の公開鍵を保存し、

送信側の電子データ保管装置が、自電子データ保管装置内に保管され、前記個別鍵を用いて暗号処理されている電子データを該公開鍵によって暗号処理し直して、該電子データを送信し、

受信側の電子データ保管装置が受信した電子データを該公開鍵と対となる秘密鍵を用いて検証し、

検証の結果、電子データが正しければ、該電子データを前記個別鍵を用いて暗号処理し直して保管することを特徴とする請求項 17 記載の電子データ保管方法。

【請求項 20】 電子データ保管装置において使用される記憶媒体であって、

保管されている電子データを自装置に固有の個別鍵を用いて検証させる機能と、

該検証の結果が正しければ、該電子データを該電子データ受信側と共通の共通鍵を用いて暗号処理し直して受信側に送信させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体。

【請求項 21】 電子データ保管装置において使用される記憶媒体であって、

外部から受信した電子データを該電子データ送信側と共通の共通鍵を用いて検証させる機能と、

該検証の結果が正しければ該電子データを自装置に固有の個別鍵を用いて暗号処理し直して保管させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は電子文書の安全性に

係り、更に詳しくはローカルな環境とグローバルな環境とにおいて、文書としての電子データの暗号処理に用いる鍵を変えることによって、電子データの安全性を確保する鍵管理機能付電子データ保管装置、および電子データ保管方法に関する。

【0002】

【従来の技術】企業間における電子商取引などの進展、公共分野の電子化等に伴い、契約書や戸籍謄本などの重要文書の電子化、ネットワーク化が本格化しようとしている。

【0003】一般の契約や更新手続きでは、書類の原本（契約書、申請書、領収書等）と、その写し（謄本、抄本等）が必要になることがよくある。紙媒体では原本と写しは明確に区別ができる。これは原本と写しとは、用紙やインクの物理的な性質が異なるためである。同様の理由で原本の改ざんも困難であった。

【0004】しかし電子文書は一般に簡単に複製を行うことができ、2つの電子文書が同じ内容を持ちながら存在することになるため、どちらが本物の原本か分からなくなるなどの問題がおこる。そのため一旦電子化処理された重要文書をわざわざ紙に印刷して保管したり、郵送したりしなければならないというような事態も存在した。

【0005】また重要文書を電子文書のままで保管したり移動したりする場合には、従来は電子データの保管装置に共通なアルゴリズムを用いて、文書を構成する電子データに対する暗号処理を行って安全性を確保するという方法がとられている。このアルゴリズムに用いられる鍵の種類は大きく2つに区別することができる。一方は電子データの送信者と受信者で共通な鍵を用いる慣用暗号であり、もう一方は公開鍵と秘密鍵の対を用いる公開鍵暗号である。

【0006】

【発明が解決しようとする課題】このように従来においては、例えば同一種類の電子データを保管する電子データ保管装置相互間、すなわちローカルな環境と、異なる種類の電子データを保管し、不特定多数の電子データ保管装置相互間で通信を行うグローバルな環境とでは、暗号処理に使用される鍵を変えることによって電子文書の安全性を確保していたが、電子データ保管装置において共通なアルゴリズムを用いているために、グローバルな環境でも電子データ保管装置に共通な鍵を用いてしまったり、ローカルな環境でも公開鍵を用いてしまうような運用が行われることがあった。

【0007】このためローカルな環境のみにおいて使用される電子データ保管装置に対しても公開鍵の運用に必要な認証局を運営してしまったり、グローバルな環境において電子データ保管装置に共通な鍵が暴露してしまうことによって全ての重要文書の信頼性が失われてしまうという問題があった。

【0008】本発明の目的は、電子データ保管装置に電子データを保管する時にはその保管装置に固有の個別鍵を用いて電子データに対する暗号処理を行い、他の電子データ保管装置との間で電子データの送受信を行う場合にはローカルな環境、またはグローバルな環境にそれぞれ適合した共通鍵を用いて暗号処理を行って電子データの送受信を行うことによって、それぞれの環境にあった鍵管理を実現できる鍵管理機能付電子データ保管装置を提供することである。

10 【0009】本発明の他の目的は、個別鍵を用いて暗号処理されている電子データを共通鍵で暗号化処理し直して、他の電子データ保管装置との間で電子データの送受信を行うことにより、電子データの安全性を確保することができる電子データ保管方法を提供することである。

【0010】

【課題を解決するための手段】図1は本発明の原理構成ブロック図である。同図は電子データを保管する時には自装置に固有の個別鍵を用いて電子データを暗号処理して保管し、他の電子データ保管装置との間でデータ送受信を行う時にはローカルな環境、またはグローバルな環境にそれぞれ適合した共通鍵を用いてデータ送受信を行う鍵管理機能付電子データ保管装置1の原理構成ブロック図である。

20 【0011】図1において、鍵管理手段2は自装置に固有の個別鍵と、他の電子データ保管装置との間で共通の共通鍵とを管理するものであり、例えば鍵管理部である。

30 【0012】暗号処理手段3は、自装置内に保管する電子データに対しては個別鍵を用いて暗号処理を行い、他の電子データ保管装置との間で送受信する電子データに対しては共通鍵を用いた暗号処理、またはデータ検証を行うものであり、例えば暗号処理部である。

【0013】本発明の実施の形態においては、鍵管理手段2によって管理される共通鍵は、複数の電子データ保管装置によって構成される1つのグループ内で共通のグループ鍵とすることも可能である。

40 【0014】この時、1つのグループ内に主となる電子データ保管装置が存在し、その保管装置の暗号処理手段3が、自装置の個別鍵を用いてその1つのグループ内の個々の電子データ保管装置の個別鍵を生成し、その生成された個別鍵が個々の電子データ保管装置に配布されることも、また同様にグループ鍵が生成されて配布されることも可能であり、グループ鍵が主となる電子データ保管装置にあらかじめ割り当てられている鍵と、新たに外部から指定される鍵とが関連づけられて生成されて、配布されることも可能である。

50 【0015】さらに複数のグループ内の主となる電子データ保管装置のそれぞれを管理するグループ管理用電子データ保管装置が存在し、その保管装置の暗号処理手段3が、自装置の個別鍵を用いて主となる電子データ保管

装置のそれぞれの個別鍵を生成して、生成された個別鍵が主となる電子データ保管装置に配布されることも可能である。

【0016】次に鍵管理手段2は、グループ鍵に加えて、自装置が属するグループと異なるグループに属する電子データ保管装置との間でのデータ送受信に用いるための公開鍵を、通信用の鍵として管理することもできる。

【0017】本発明の実施の形態においては、鍵管理手段2が個別鍵と共通鍵とに加えて、全ての電子データ保管装置に共通のマスタ鍵を管理することもできる。

【0018】この時各電子データ保管装置の暗号処理手段3は、このマスタ鍵を用いて自装置を識別する情報を暗号化して個別鍵を生成することもでき、また1つのグループ内に主となる電子データ保管装置が存在する場合には、その保管装置の暗号処理手段3が自装置内で生成した個別鍵を用いてそのグループを識別する情報を暗号化してグループ鍵を生成し、生成されたグループ鍵がそのグループに属する個々の電子データ保管装置に配布されることも可能である。

【0019】さらに本発明の実施の形態においては、それぞれ複数の電子データ保管装置によって構成されるグループを1つの階層とする階層構造が構成され、鍵管理手段2が自装置が属するグループの階層に応じたグループ鍵を共通鍵として管理することもでき、またこの階層構造において上位側の階層のグループ内に、直近下位の階層のグループの電子データ保管装置を管理する管理用電子データ保管装置が存在し、その管理用電子データ保管装置が自装置の個別鍵を用いて直近下位の階層に対応するグループ鍵を生成し、生成されたグループ鍵が直近下位の階層の電子データ保管装置に配布されるようにすることも可能である。

【0020】次に本発明の電子データ保管方法においては、他の電子データ保管装置との間で共通の共通鍵を用いて電子データの通信が行われ、自装置に保管すべきデータに対しては、自装置に固有の個別鍵を用いて暗号処理が行われる。

【0021】本発明の実施の形態としての電子データ保管方法においては、共通鍵として複数の電子データ保管装置によって構成される1つのグループ内で共通のグループ鍵が保持され、送信側の電子データ保管装置内でその装置固有の個別鍵を用いて暗号処理されている電子データが、グループ鍵によって暗号処理し直されて送信され、受信側の電子データ保管装置によって受信された電子データがグループ鍵を用いて検証され、検証の結果電子データが正しければ、その電子データが受信側の装置に固有の個別鍵を用いて暗号処理し直して保管されることもできる。

【0022】また、本発明の実施の形態としての電子データ保管方法においては、共通鍵として自装置が属する

グループと異なる他のグループに属する電子データ保管装置の公開鍵が保持され、送信側の装置が自装置内に保持され、個別鍵を用いて暗号処理されている電子データを公開鍵によって暗号処理し直して送信し、受信側の装置が受信した電子データを公開鍵と対となる秘密鍵を用いて検証し、検証の結果が正しければ、その電子データを受信側の電子データ保管装置に固有の個別鍵を用いて暗号処理し直して保管するようにすることも可能である。

【0023】また本発明の電子データ保管装置において使用される記憶媒体として、保管されている電子データを自装置に固有の個別鍵を用いて検証させる機能と、検証の結果が正しければ、その電子データを受信側と共通の共通鍵を用いて暗号処理し直して送信させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体を用いることもできる。

【0024】また電子データ保管装置において使用される記憶媒体として、外部から受信した電子データを送信側と共通の共通鍵を用いて検証させる機能と、その検証の結果が正しければ、その電子データを自装置に固有の個別鍵を用いて暗号処理し直して保管させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体を用いることもできる。

【0025】以上のように本発明によれば、自装置に保管すべき電子データに対しては自装置に固有の個別鍵を用いて暗号処理を行い、また他の電子データ保管装置との間で送受信する電子データに対しては、相手側の装置との間で共通の共通鍵を用いて電子データの暗号処理と、その検証が行われる。

【0026】

【発明の実施の形態】図2は本発明の第1の実施形態における鍵管理機能付電子データ保管装置の構成ブロック図である。本発明の第1の実施形態においては、電子データ保管装置10の内部には個別鍵、グループ鍵、および公開鍵の3種類の鍵が保持される。

【0027】図2において制御部11は全体の動作を制御するものである。鍵管理部12は電子データ保管装置10の内部に保持されている鍵を管理するものであり、暗号処理部13は必要に応じて鍵を生成したり、電子データを暗号化したり、電子データを検証する処理を行うものである。

【0028】個別鍵保持部14はその電子データ保管装置10に固有の個別鍵を保持し、グループ鍵保持部15は複数の電子データ保管装置10によって構成される1つのグループ内での共通鍵としてのグループ鍵を保持するものであり、公開鍵保持部16は、例えば他のグループに属する電子データ保管装置10との間で電子データの送受信を行う場合に使用される公開鍵を保持するものである。

【0029】電子データ保管装置10の内部には、更に

10

20

30

40

50

電子データを保管するデータ保管部 17 と、他の電子データ保管装置との間で電子データの送受信を行うための通信処理部 18 が備えられている。通信処理部 18 はネットワークとして接続されている。

【0030】図 3 は本発明の第 1 の実施形態における電子データ保管装置の全体処理フローチャートである。同図において、ステップ S 1 で電子データが入力されるか、または例えば電子データの送信指示が入力されると、ステップ S 2 で電子データ保管装置へのデータ保存か否かが判定される。なおステップ S 1 での送信指示は保管装置の利用者、またはアプリケーションから、例えばネットワークを介して与えられる。

【0031】データの保存である場合には、ステップ S 3 で鍵管理部 12 によって個別鍵保持部 14 が保持する個別鍵が選択され、ステップ S 4 で個別鍵を用いて暗号処理部 13 によって電子データに対する暗号処理が行われ、ステップ S 5 でデータ保管部 17 にデータが保管されて処理を終了する。

【0032】ステップ S 2 でデータの保存でない場合には、ステップ S 6 で、ステップ S 1 で与えられた指示がグループ内の電子データ保管装置との間でのデータの送受信か否かが判定され、グループ内のデータ送受信である場合には、ステップ S 7 で鍵管理部 12 によってグループ鍵保持部 15 が保持するグループ鍵が選択され、ステップ S 8 で暗号処理部 13 によってグループ鍵を用いて電子データに対する暗号処理が行われ、ステップ S 9 で通信処理部 18 から電子データの送信が行われて、処理を終了する。

【0033】ステップ S 6 でグループ内のデータ送受信でない場合には、ステップ S 11 で異なるグループに属する電子データ保管装置との間でのデータの送受信であるか否かが判定され、データ送受信でない場合にはそのまま処理を終了する。異なるグループに属する電子データ保管装置との間でのデータ送受信である場合には、ステップ S 12 で鍵管理部 12 によって公開鍵保持部 16 から公開鍵が選択され、ステップ S 8 で公開鍵を用いて暗号処理が行われ、ステップ S 9 でデータが送信されて、処理を終了する。

【0034】図 4 は、図 3 におけるグループ内データ送受信処理の詳細フローチャートである。同図において、ステップ S 15 で送信側の電子データ保管装置に対してグループ内通信指示が与えられると、ステップ S 16 でデータ保管部 17 から送信すべきデータが選択され、ステップ S 17 で鍵管理部 12 によって個別鍵保持部 14 の保持する個別鍵が選択され、ステップ S 17 で鍵管理部 12 によって個別鍵保持部 14 の保持する個別鍵が選択され、ステップ S 18 で暗号処理部 13 によって個別鍵を用いて電子データの復号とその内容の検証が行われる。この暗号処理部による処理については後述する。

【0035】電子データ検証の結果、電子データの改ざ

んが行われていないことが判明すれば、ステップ S 19 で鍵管理部 12 によってグループ鍵保持部 15 に保持されているグループ鍵が選択され、ステップ S 20 で暗号処理部 13 によってグループ鍵を用いて電子データに対する暗号処理が行われ、ステップ S 21 で通信処理部 18 によって受信側の電子データ保管装置に対するデータ送信が行われる。

【0036】受信側の電子データ保管装置においては、通信処理部 18 によってステップ S 24 でデータが受信され、ステップ S 25 で鍵管理部 12 によってグループ鍵保持部 15 が保持するグループ鍵が選択され、ステップ S 26 で暗号処理部 13 によってグループ鍵を用いて電子データの復号とその内容の検証が行われる。

【0037】検証の結果、電子データが改ざんされていないことが判明すると、ステップ S 27 で鍵管理部 12 によって個別鍵保持部 14 が保持する個別鍵が選択され、ステップ S 28 で暗号処理部 13 によって個別鍵を用いて電子データに対する暗号処理が行われ、ステップ S 29 でデータ保管部 17 にデータが保管されて、処理を終了する。

【0038】図 5 は異なるグループに属する電子データ保管装置との間での電子データ送受信の詳細処理フローチャートである。図 4 のグループ内の電子データ保管装置との間でのデータ送受信の処理フローチャートと異なる部分を中心に説明する。まず送信側の電子データ保管装置において、ステップ S 31 で異なるグループに属する電子データ保管装置との間での通信指示が受け取られ、図 4 におけると同様にステップ S 16 ~ S 18 の処理が行われる。その後ステップ S 32 で鍵管理部 12 によって公開鍵保持部 16 に保持されている公開鍵が選択され、ステップ S 33 でその公開鍵を用いて暗号処理が行われ、その結果はステップ S 21 で受信側の電子データ保管装置に向けて送信される。

【0039】受信側の電子データ保管装置においては、ステップ S 24 でデータを受信した後、ステップ S 36 で鍵管理部 12 によって公開鍵保持部 16 に保持されている公開鍵と対となる秘密鍵が選択され、ステップ S 37 で暗号処理部 13 によって公開鍵暗号アルゴリズムを用いてデータの復号、および内容の検証が行われる。電子データの改ざんが行われていないことが検証されると、図 4 におけると同様にステップ S 27 ~ S 29 の処理が行われ、処理を終了する。ここで電子文書には送信側の秘密鍵による電子署名と受信側の公開鍵による暗号文を同時に送るような PEM (プライバシ・エンハンスド・メール) のような一般的な方法を用いてもよい、送信側と受信側の公開鍵によって、D-H 法 (ディフィー・ヘルマン法) によってセッション鍵を一時的に共有して通信を行ってもよい。

【0040】図 4、および図 5 で説明したように、グループ内、または異なるグループに属する電子データ保管

装置との間でデータの送受信を行う場合には、送信側において個別鍵によって暗号処理されて保管されているデータを、グループ内ではグループ鍵、異なるグループの場合には公開鍵によって暗号処理をし直して送信し、受信側ではグループ内ではグループ鍵、異なるグループとの間では公開鍵を用いてデータの検証を行った後、個別鍵で暗号処理し直して保管することによって、例えばグループ鍵が暴露されると危険に犯されたとしても、各保管装置内部に保管されている電子データの安全性を保つことが可能となる。

【0041】続いて各電子データ保管装置に保持されている鍵の生成、および管理について、図6～図10を用いて、その処理フローチャートを説明する。図6は各電子データ保管装置の個別鍵があらかじめ割り当てられている場合のデータ保管処理のフローチャートである。あらかじめ電子データ保管装置に割り当てられている鍵とは、例えば電子データ保管装置の工場出荷時に各装置に割り当てられる鍵のことであり、メーカーによって管理されるため、メーカー鍵と呼ぶことにする。

【0042】図6において、工場出荷時にステップS40でメーカーによって鍵管理機能付電子データ保管装置が作成されて、ステップS41でメーカーによってその電子データ保管装置に対するメーカー鍵が作成され、ステップS42でそのメーカー鍵が個別鍵保持部14に設定された後、電子データ保管装置が出荷される。このメーカー鍵は電子データ保管装置の識別情報、例えばIDなどと組み合わせ、メーカーによって管理される。

【0043】電子データ保管装置の利用時には、ステップS44で電子データが受信され、ステップS45で鍵管理部12によって個別鍵保持部14に保持されているメーカー鍵が選択され、ステップS46で暗号処理部13によってメーカー鍵を用いて電子データの暗号処理が行われ、ステップS47でデータ保管部17にデータが保管されて、処理を終了する。

【0044】このように電子データ保管装置の個別鍵としてメーカーによって管理されるメーカー鍵を用いることによって、利用者は鍵の管理をする必要がなくなり、また利用者側での鍵の暴露を最小限にすることができる。また利用者側の電子データ保管装置の暗号処理部13が壊れても、メーカーによって管理されているメーカー鍵を用いて電子データ保管装置内のデータを再構築することも可能となる。

【0045】図7はグループの中の主となる電子データ保管装置、例えばグループマスタによるグループ内の電子データ保管装置の個別鍵の管理処理のフローチャートである。同図において処理が開始されると、まずステップS50で複数の電子データ保管装置によって構成されるグループの中で主となる保管装置、例えばグループマスタが決定され、S51でそのグループマスタの鍵を用いてグループに属する個々の保管装置の個別鍵が作成さ

れ、ステップS52でグループマスタが作成した個々の保管装置の個別鍵が配布され、ステップS53で個々の電子データ保管装置は個別鍵保持部14に配布された鍵を設定して、処理を終了する。グループマスタによる各個別鍵の生成、およびその配布の方法については後述する。

【0046】図8は2つの鍵を関連付けて個別鍵を生成する処理のフローチャートである。2つの鍵とは、例えば電子データ保管装置にあらかじめ割り当てられている鍵と、新たに指定される鍵であり、あらかじめ割り当てられている鍵は、例えば前述のメーカー鍵であり、新たに指定される鍵とは電子データ保管装置を利用する管理者によって設定される鍵であり、管理者鍵と呼ばれるものである。管理者は利用者（ユーザ）と異なって、個別鍵、グループ鍵の設定をすることができるが、利用者は、電子データの保管、参照、および転送などしか行うことができない。

【0047】図8において、ステップS55で管理者によって新たに個別鍵の生成の指示が与えられると、ステップS56で管理者によって管理者鍵が指定され、ステップS57で暗号処理部13によって前述のメーカー鍵と管理者鍵とが関連づけられて個別鍵が生成され、ステップS58で鍵管理部12によって個別鍵保持部14に生成された個別鍵が設定されて、処理を終了する。メーカー鍵と管理者鍵との関連づけによる個別鍵の生成については後述する。

【0048】このように電子データ保管装置の個別鍵の生成にあたってメーカー鍵と管理者鍵とを関連づけることにより、管理者が組織の変更やグループの構築など、環境や運用形態に合わせて、電子データ保管装置を管理することができる。また暗号処理部が壊れた場合などに、前述と同様にメーカーがデータの再構築や検証を行うことも可能である。

【0049】図9はグループマスタによるグループ鍵管理処理のフローチャートである。グループ鍵は、前述のように1つのグループ内での電子データの送受信に対して用いられるものであり、図9のフローチャートは図7のグループマスタによる個別鍵の管理処理のフローチャートと同様である。

【0050】すなわちステップS60でグループマスタが決定された後、ステップS61でグループマスタによってグループ鍵が生成され、ステップS62でそのグループ鍵がグループ内の電子データ保管装置に配布され、ステップS63で各電子データ保管装置はグループ鍵保持部15に配布されたグループ鍵を設定して、処理を終了する。

【0051】図10は、図8と同様に、2つの鍵を関連づけてグループ鍵を生成する処理のフローチャートである。図8における同様に、2つの鍵とはメーカー鍵と管理者鍵のことである。

【0052】図10の最初の2つのステップは図8におけると同様である。その後、ステップS66で暗号処理部13によってメーカ鍵と管理者鍵とが関連づけられてグループ鍵が生成され、ステップS67で鍵管理部12によってグループ鍵保持部15にグループ鍵が設定され、ステップS68でグループに属する電子データ保管装置にグループ鍵が配布されて、処理を終了する。なおこのフローチャートの処理は、例えば前述のグループマスタによって行われるものである。

【0053】図11は本発明の第2の実施の形態における鍵管理機能付電子データ保管装置の構成ブロック図である。第1の実施の形態における図2と比較すると、全ての電子データ保管装置に共通の鍵であるマスタ鍵を保持するマスタ鍵保持部20が追加されている点だけが異なっている。

【0054】図12は第2の実施の形態におけるマスタ鍵を用いた個別鍵生成処理のフローチャートである。同図において、ステップS70で個別鍵の生成指示を受け取ると、ステップS71で制御部11によって自装置の識別情報、例えば電子データ保管装置のIDが取得され、ステップS72で鍵管理部12によってマスタ鍵保持部20に保持されているマスタ鍵が取得され、ステップS73で暗号処理部13によって電子データ保管装置識別情報がマスタ鍵を用いて暗号化されて、個別鍵が生成される。この暗号化処理については後述する。そして、ステップS74で鍵管理部12によって、個別鍵保持部14に生成された個別鍵が設定されて処理を終了する。

【0055】このように全ての電子データ保管装置に共通のマスタ鍵を用いて個々の電子データ保管装置が個別鍵を生成することによって、個々の保管装置による自動的な個別鍵生成が可能となる。また電子データ保管装置のメーカは、暗号処理部が壊れた時などに電子データ保管装置の識別情報を参照することにより、保管されているデータ検証や再構築を行うことが可能となる。

【0056】図13は第2の実施の形態におけるグループ鍵生成とその配布処理のフローチャートである。なおこの処理ではマスタ鍵は使用されないため、第1の実施の形態においても同様の処理を実行することが可能である。

【0057】図13のステップS75でグループ鍵作成指示がグループマスタに与えられると、ステップS76でグループマスタの制御部11によってグループ識別情報が取得される。このグループ識別情報は、そのグループマスタが管理するグループを識別するためのIDである。そしてS77で鍵管理部12によって個別鍵保持部14に保持されている個別鍵が選択され、ステップS78で暗号処理部13によってグループ識別情報が個別鍵で暗号化されてグループ鍵が生成され、ステップS79で生成されたグループ鍵が通信処理部18からグループ

内の電子データ保管装置に配布される。

【0058】グループマスタによって管理される、グループに属する保管装置側では、ステップS80aにおいて通信処理部18によってグループ鍵が受信され、ステップS80bで鍵管理部12によってグループ鍵保持部15にグループ鍵が設定されて処理を終了する。

【0059】図14はグループ管理電子データ保管装置によるグループマスタの個別鍵生成処理のフローチャートである。グループ管理電子データ保管装置とは、複数のグループ内でそれぞれ主となる電子データ保管装置、すなわち複数のグループマスタを管理するものであり、グループ管理電子データ保管装置はグループマスタを管理するものであり、グループ管理電子データ保管装置はグループマスタ個々に対する個別鍵を生成して、グループマスタに配布する。

【0060】ステップS82でグループマスタの個別鍵の生成指示が受け取られ、ステップS83で複数の各グループに対するグループ識別情報が指定され、ステップS84で鍵管理部12によって個別鍵保持部14に保持されている個別鍵が選択され、ステップS85で暗号処理部13によって個別鍵を用いて各グループ識別情報が暗号化され、各グループマスタに対する個別鍵が生成され、ステップS86で各グループマスタに個別鍵が配布されて、処理を終了する。

【0061】次にグループの階層化について説明する。例えば図3では、それぞれ複数の電子データ保管装置によって構成される複数のグループはお互いに対等なものとして、本発明の第1の実施形態、および第2の実施形態を説明したが、グループの間に上位のグループと下位のグループとの階層関係が存在する場合を図15に示す。

【0062】図15において、上位グループは管理グループとしての下位のグループを管理しており、上位グループに属する電子データ保管装置(SA)は、例えば自グループに対する上位グループ鍵と、管理グループに対する下位グループ鍵を保持しているものとする。これに対して下位グループに属する電子データ保管装置は自グループに対する下位グループだけを保持するものとする。そして例えば上位グループの中で、下位グループの電子データ保管装置を管理する下位グループマスタSAが、下位グループ鍵を作成して、下位グループのSAに配布するものとする。ここでSAはセキュア・アーカイバの略号であり、電子データ保管装置である。

【0063】図16は階層関係にある2つのグループにおける通信方法の説明図である。上位グループの中でのSA同志の通信は上位グループ鍵を用いて行われ、下位グループの中でのSA同志の通信は下位グループ鍵を用いて行われる。上位グループのSA、例えばSA1と下位グループのSA、例えばSA2との間の通信は上位グループ中のSAの1つであり、下位グループのSAを管

理する下位グループマスタSAを介して行われるものとする。下位グループマスタSAと下位グループに属するSA、例えばSA2との間の通信は下位グループ鍵を用いて行われるものとする。

【0064】この下位グループマスタSAがある組織の管理部に属しているものとすれば、管理部のSAが各部門等のSAの個別鍵やグループ鍵を生成、配布、管理することによりグループの階層化が実現され、また各SAに保管されているデータを管理部から検証することが可能となる。

【0065】図17は、図16において、例えば上位グループのSA1から下位グループのSA2への通信処理のフローチャートである。同図において、ステップS91で上位グループのSA1に対して下位グループのSA2に対するデータの転送が指示されると、ステップS92で、例えば図2の鍵管理部12によって個別鍵保持部14の保持する個別鍵が選択され、ステップS93で暗号処理部13によって個別鍵を用いてデータの復号と検証が行われ、ステップS94で鍵管理部12によってグループ鍵保持部15に保持されている上位グループ鍵が選択され、ステップS95で暗号処理部13によって上位グループ鍵を用いて電子データに対する暗号処理が行われ、ステップS96で通信処理部18から暗号処理された電子データが下位グループマスタSAに転送される。

【0066】下位グループマスタSA側では、ステップS97で通信処理部18によって暗号処理されたデータが受信され、ステップS98で鍵管理部12によってグループ鍵保持部15に保持されている上位グループ鍵が選択され、ステップS99で暗号処理部13によって上位グループ鍵を用いて電子データの復号と検証が行われ、ステップS100で鍵管理部12によってグループ鍵保持部15に保持されている下位グループ鍵が選択され、ステップS101で暗号処理部13によって下位グループ鍵を用いてデータに対する暗号処理が行われ、ステップS102で通信処理部18によって暗号処理されたデータが下位グループのSA2に転送される。

【0067】下位グループのSA2においては、ステップS103で通信処理部18によって暗号処理されたデータが受信され、ステップS104で鍵管理部12によってグループ鍵保持部15に保持されている下位グループ鍵が選択され、ステップS105で暗号処理部13によって下位グループ鍵を用いてデータの復号と検証が行われ、ステップS106で鍵管理部12によって個別鍵保持部14に保持されている個別鍵が選択され、ステップS107で暗号処理部13によって個別鍵を用いてデータに対する暗号処理が行われ、ステップS108で制御部11によってデータ保管部17にデータが保管されて、処理を終了する。

【0068】図18は、図17とは逆に、下位グループ

のSA2から上位グループのSA1へのデータ送信処理のフローチャートである。同図の処理は図17とは逆になるだけであり、データ送信側のSA2では個別鍵と下位グループ鍵を用いて処理が行われ、下位グループマスタSAでは下位グループ鍵を用いてデータの復号と検証が行われた後、上位グループ鍵を用いてデータに対する暗号処理が行われ、受信側のSA1では上位グループ鍵と個別鍵とを用いて処理が行われることになる。

【0069】なお図17の説明に図2の第1の実施の形態における電子データ保管装置の構成を用いたが、図17および図18の処理は、図11で説明した第2の実施の形態における電子データ保管装置においても全く同様に行われる。

【0070】次に個別鍵を用いた電子データ（電子文書）の保管、グループ内におけるグループ鍵の利用方法、電子データに対する改ざん検出情報（MAC、メッセージオーセンティフィケーションコード）の作成、鍵の生成などについて説明する。

【0071】図19は個別鍵を利用した電子文書保管の説明図である。同図において、①で電子文書の保管指示が電子データ保管装置に与えられると、保管装置において②で個別鍵と電子文書を用いてMACが構成され、③でMACと電子文書が保管される。

【0072】図20は同一グループ内の2つの電子データ保管装置AとBの間での通信方法の説明図である。同図において、送信側のデータ保管装置A側では、①でMACの再計算が行われて、電子文書の検証が行われた後に、②でグループ鍵と電子文書に対応してMACが計算され、③でそのMACと電子文書が保管装置B側に送信される。

【0073】電子データ保管装置B側では、④でMACと電子文書を受信し、⑤でMACの内容をグループ鍵を用いて検証し、検証結果が正しければ、⑥で個別鍵と電子文書に対応してMACが計算され、⑦で計算されたMACと電子文書が保管される。

【0074】図21は、図19、図20で説明した電子データに対する改ざん検出情報MACの計算方法の説明図である。MACの計算においては、アメリカの規格協会によって採用された暗号化法としてのDES（データエンクリプションスタンダード）が用いられる。この暗号化法では、暗号化／復号化を1つのLSIで処理することができる。

【0075】図21において、まず元データが64ビットずつのブロックM1、M2、・・・Mnに分割される。そして、まず最初のブロックM1、64ビットに対するDES処理が、鍵、例えば個別鍵を用いて行われ、その結果の64ビットのデータと次のブロックM2、64ビットとの排他的論理和が求められる。

【0076】さらにその結果に対して、例えば個別鍵を用いて再びDES処理が行われ、64ビットの結果が得

られる。以後同様の処理が行われ、最終的に得られる 64 ビットのうちで、上位 32 ビットが改ざん検出情報 MAC として求められる。なお改ざん検出情報 MAC の計算は、ここで示した方法に限定されるものではなく、他のアルゴリズムを用いてもよい。

【0077】図 22 は一般的な鍵の生成法の説明図である。同図において、例えば前述のグループマスタがグループに属する電子データ保管装置の個別鍵を生成して配布する場合には、個々の保管装置を識別する情報、例えば ID とシード鍵としてのグループマスタの個別鍵を用いて DES 処理を行い、個々の保管装置に対応する個別鍵を、ニュー鍵として生成して配布することができる。前述のように例えばメーカ鍵と管理者鍵の 2 つの鍵を関連づけて新たな鍵を生成する場合も全く同様である。

【0078】この個別鍵の配布の方法としては、鍵配布サーバを用いたり、公開鍵をベースとした認証基盤に基づく GKM F (グループキーマネジメントフレームワーク) を用いてオンラインで配布してもよく、フロッピーや IC カードなどの媒体を用いてオフラインで配布することもできる。

【0079】ここで、GKM F は公開鍵認証基盤の証明書を各グループメンバが持つことによって鍵の設定や更新等の管理を行うものである、また公開鍵をベースとした認証基盤とは信頼のおける第 3 者としての認証局を信頼点とすることによって、各個人が公開鍵に対して第 3 者のお墨付き (電子署名) を受けることによって、2 者の間の認証を行う枠組みである。

【0080】図 23 はグループ鍵の生成とその配布の説明図である。同図において、2 つのグループ 1、2 が存在し、各グループはグループマスタの配下に、例えば 3 つの SA を備えているものとする。図 23 では、例えばグループマスタは自装置の個別鍵、I 鍵と自装置の ID とを用いて、まずグループマスタ鍵 (G_m 鍵) を生成し、その後この G_m 鍵とグループに対する ID を用いてグループ鍵、G 鍵を生成し、このグループ鍵を配下の SA に配布する。

【0081】このグループ鍵は各 SA 内のグループ鍵保持部に保持されるが、グループ鍵はグループを識別する ID と鍵のペアで管理されており、例えば 1 つの SA が複数のグループに属したり、図 16 で説明した下位グループマスタ SA のように上位グループ鍵と下位グループ鍵とを保持する必要があるために、グループ鍵とグループを識別する ID のペアが一般に複数保持されることになる。またグループ鍵と ID のペアの他に、グループに含まれるデータ保管装置の IP アドレスや、名前などの属性を同時に管理してもよい。

【0082】また図 23 において、グループ 1 とグループ 2 の間の通信はセッション鍵 (S 鍵) を用いて行われている。このセッション鍵は、公開鍵証明書に基づいて、例えばグループマスタ相互間で共通される秘密鍵で

ある。公開鍵は、一般に異なる複数のグループとの間の通信を行うためにグループ鍵と同様に複数、例えばグループマスタによって管理され、国際電気通信連合の ITU-T X509 に示される公開鍵証明書の形式を用いて、信頼のおける第 3 者が認証を確認できる形態で、保存されてもよい。

【0083】図 24 は、それぞれ複数の SA によって構成されるグループが複数存在する場合の、グループ管理 SA による全体管理方法の説明図である。同図においてグループ A、B、C の 3 つのグループが構成されており、それぞれのグループ内で主となる電子データ保管装置、すなわちグループマスタ SA が存在する。

【0084】グループ管理 SA は (グループ管理電子データ保管装置) は各グループのグループマスタ SA を管理するものであり、例えば図 14 で説明したようにグループマスタ SA の個別鍵を生成して各グループマスタ SA に配布するような処理を実行する。このように複数のグループを管理するグループ管理 SA が存在することによって、インターネットのようなグローバルなネットワーク環境でも、不特定多数のグループのいずれのグループをも相手とする通信が可能となる。

【0085】最後に、本発明の鍵管理機能付電子データ保管装置どを実現するためのプログラムのコンピュータへのローディングについて、図 25 を用いて説明する。同図において、セキュアな筐体内のコンピュータ 25 は本体 26 とメモリ 27 とから構成されており、本体 26 に対してはセキュアな可搬型記憶媒体 29 からプログラムなどをロードすることも、またプログラム提供者側からネットワーク 28 を介してプログラムなどをロードすることも可能である。

【0086】本発明の特許請求の範囲における電子データ保管装置内の各種の処理や、電子データ保管装置相互間でのデータ送受信などのためにプログラムや、各フローチャートに示されているプログラムなどは、例えばセキュアなメモリ 27 に格納され、そのプログラムは本体 26 によって実行される。ここでセキュアなメモリ 27 としては、ハードディスクなどが用いられる。

【0087】また例えば電子ディスク保管装置相互間でのデータ送受信のためのプログラムなどは、セキュアな可搬型記憶媒体 29 に記憶され、セキュアな筐体内のコンピュータ 25 にそのプログラムをロードすることによって、通信を行うことも可能である。このセキュアな可搬型記憶媒体 29 としては、セキュアなメモ리카ード、フロッピーディスク、CD-ROM、光ディスク、光磁気ディスクなどを用いることができる。さらにデータ通信のためのプログラムなどは、プログラム提供者側からネットワーク 28 を介してセキュアな筐体内のコンピュータ 25 側に送られ、そのプログラムがロードされることによってデータの通信を実現することも可能である。

【0088】以上において本発明の実施の形態を詳細に

説明したが、本発明の実施の形態は以上の記述に限定されることなく、特許請求の範囲に記載された範囲内で様々な実施形態を取ることができることは当然である。

【0089】

【発明の効果】以上詳細に説明したように、電子データ保管装置が鍵管理機能を備えることによって、利用環境に適した電子データの保管および送受信が可能となり、電子化された重要文書の安全性確保に寄与することが大きい。

【図面の簡単な説明】

【図1】本発明の原理構成ブロック図である。

【図2】本発明の第1の実施の形態における電子データ保管装置の構成を示すブロック図である。

【図3】第1の実施の形態における電子データ保管装置の全体処理フローチャートである。

【図4】同一グループに属する電子データ保管装置との間でのデータ送受信処理のフローチャートである。

【図5】異なるグループに属する電子データ保管装置との間でのデータ送受信処理のフローチャートである。

【図6】個別鍵があらかじめ割り当てられている場合の電子データ保管処理のフローチャートである。

【図7】グループマスタによる電子データ保管装置個別鍵の管理処理フローチャートである。

【図8】2つの鍵を関連付けて個別鍵を生成する処理のフローチャートである。

【図9】グループマスタによるグループ鍵管理処理のフローチャートである。

【図10】2つの鍵を関連づけてグループ鍵を生成する処理のフローチャートである。

【図11】第2の実施の形態における電子データ保管装置の構成を示すブロック図である。

【図12】第2の実施の形態におけるマスタ鍵を用いた個別鍵生成処理のフローチャートである。

【図13】第2の実施の形態におけるグループ鍵生成処理のフローチャートである。

【図14】グループ管理保管装置によるグループマスタ

の個別鍵生成処理のフローチャートである。

【図15】グループの階層化を説明する図である。

【図16】上位グループと下位グループの電子データ保管装置相互間での通信を説明する図である。

【図17】上位グループの保管装置から下位グループの保管装置へのデータ送信処理のフローチャートである。

【図18】下位グループの保管装置から上位グループの保管装置へのデータ送信処理のフローチャートである。

【図19】個別鍵を用いた電子文書保管の説明図である。

【図20】同一グループに属する2つの保管装置の間でのデータ送受信を説明する図である。

【図21】改ざん検出情報MACの計算方法を説明する図である。

【図22】鍵の生成方法の説明図である。

【図23】グループ鍵の生成とその配布を説明する図である。

【図24】それぞれ複数のSAによって構成されるグループが複数存在する場合の、グループ管理SAによる全体管理方式の説明図である。

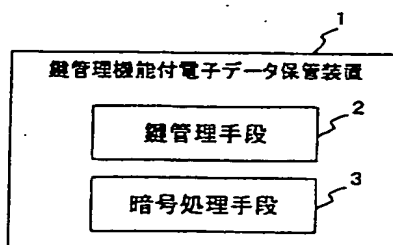
【図25】本発明の電子データ保管装置を実現するためのプログラムのコンピュータへのローディングを説明する図である。

【符号の説明】

- 1, 10, 19 鍵管理機能付電子データ保管装置
- 2 鍵管理手段
- 3 暗号処理手段
- 11 制御部
- 12 鍵管理部
- 13 暗号処理部
- 14 個別鍵保持部
- 15 グループ鍵保持部
- 16 公開鍵保持部
- 17 データ保管部
- 18 通信処理部
- 20 マスタ鍵保持部

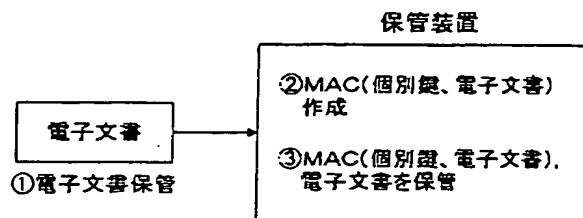
【図1】

本発明の原理構成ブロック図



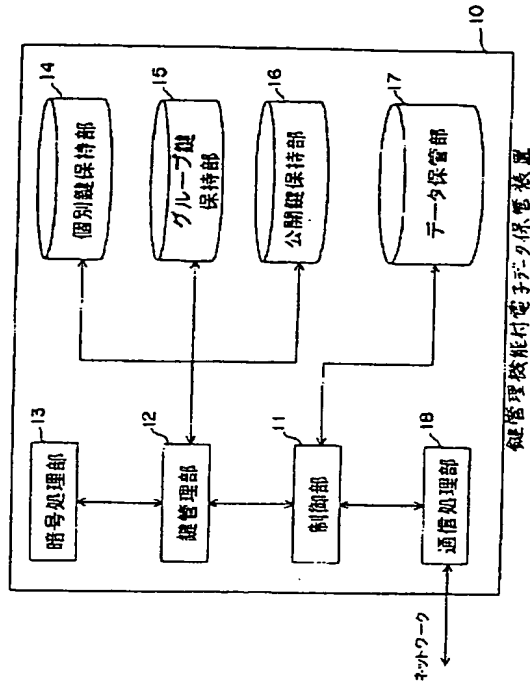
【図19】

個別鍵を用いた電子文書保管の説明図



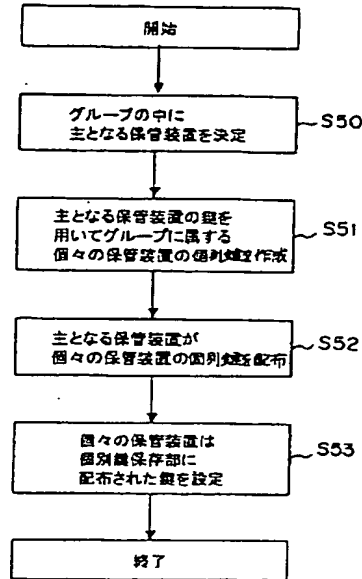
【図2】

本発明の第1の実施形態における
電子データ保管装置の構成を示すブロック図



【図7】

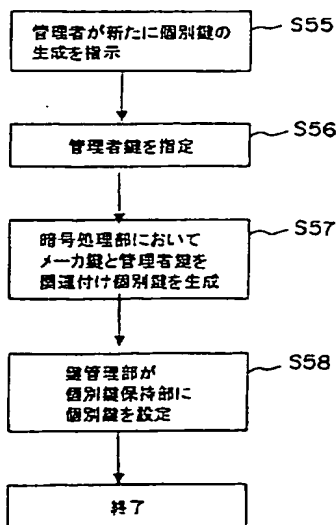
グループマスターによる電子データ
保管装置個別鍵の管理処理フローチャート



【図22】

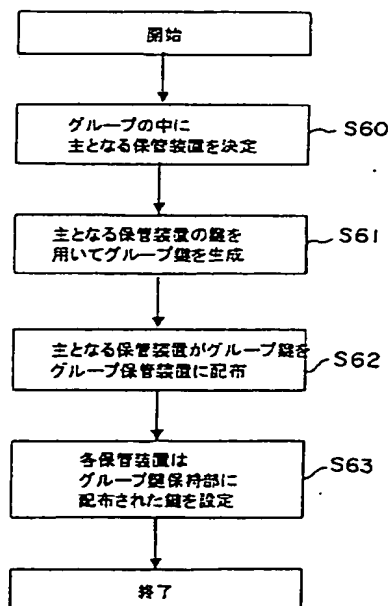
【図8】

2つの鍵を関連付けて個別鍵を
生成する処理のフローチャート

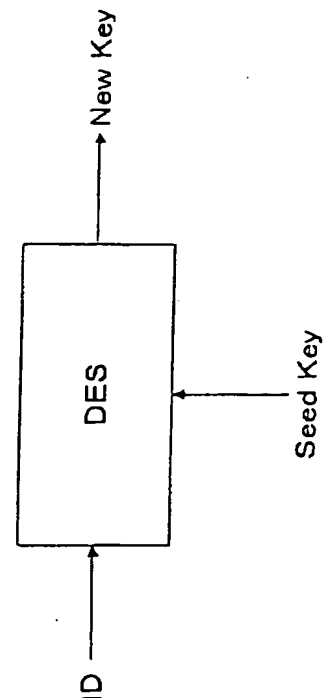


【図9】

グループマスターによるグループ鍵
管理処理のフローチャート

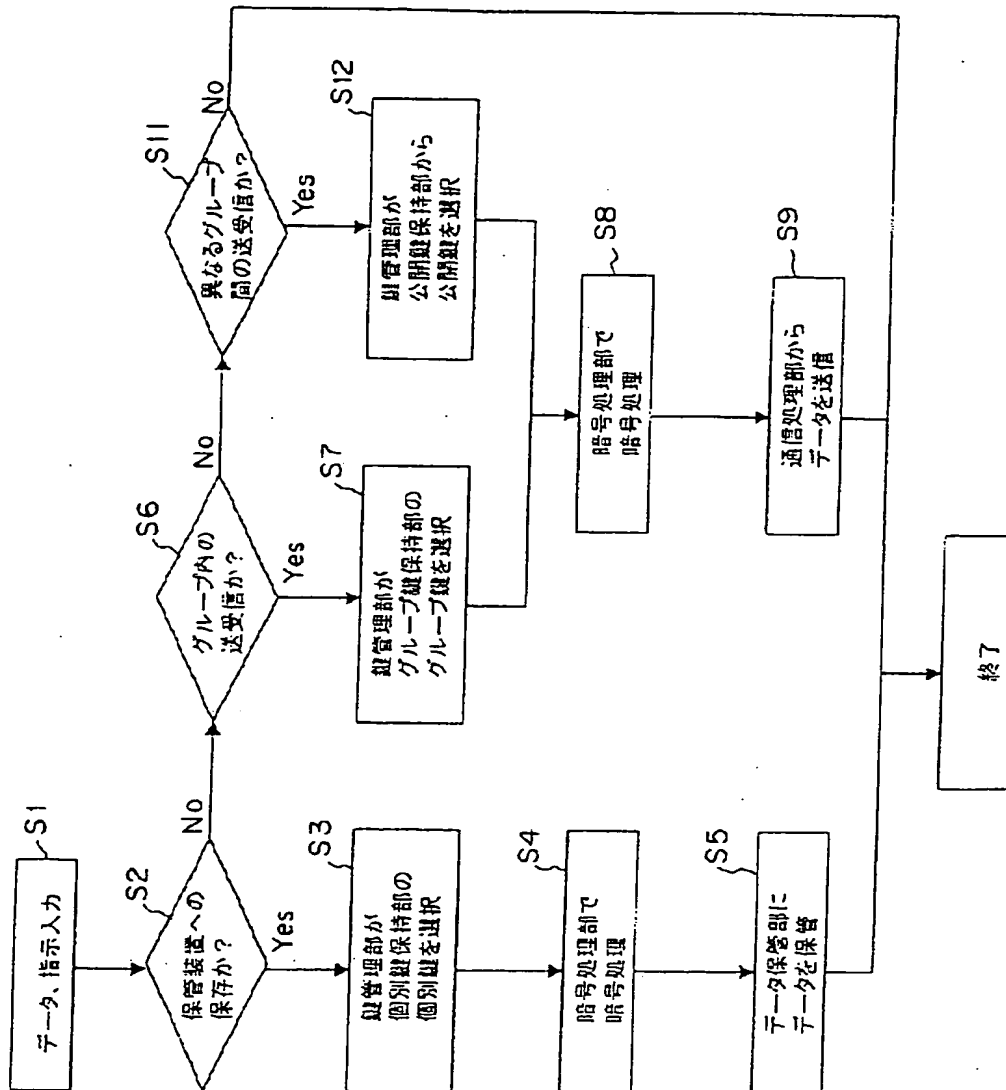


鍵の生成方法の説明図



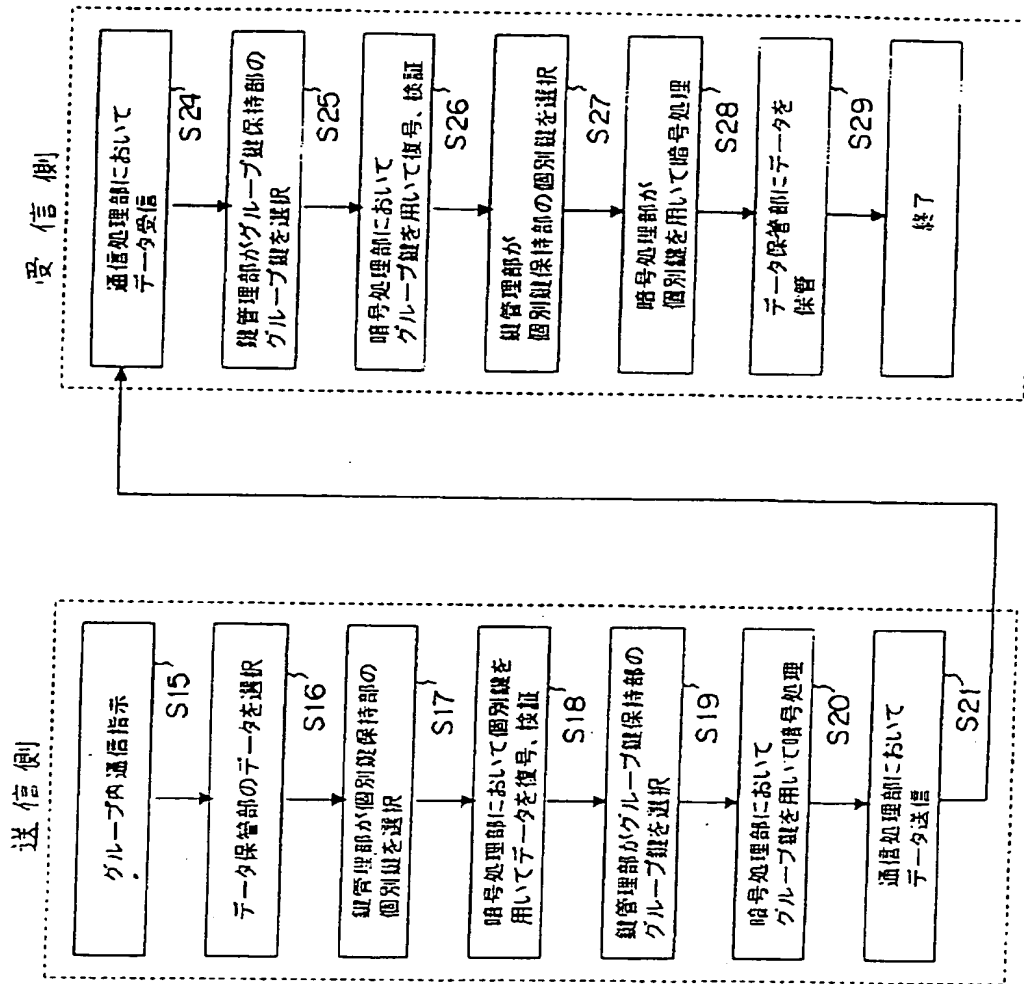
【図3】

第1の実施形態における電子データ保管装置の
全体処理フローチャート



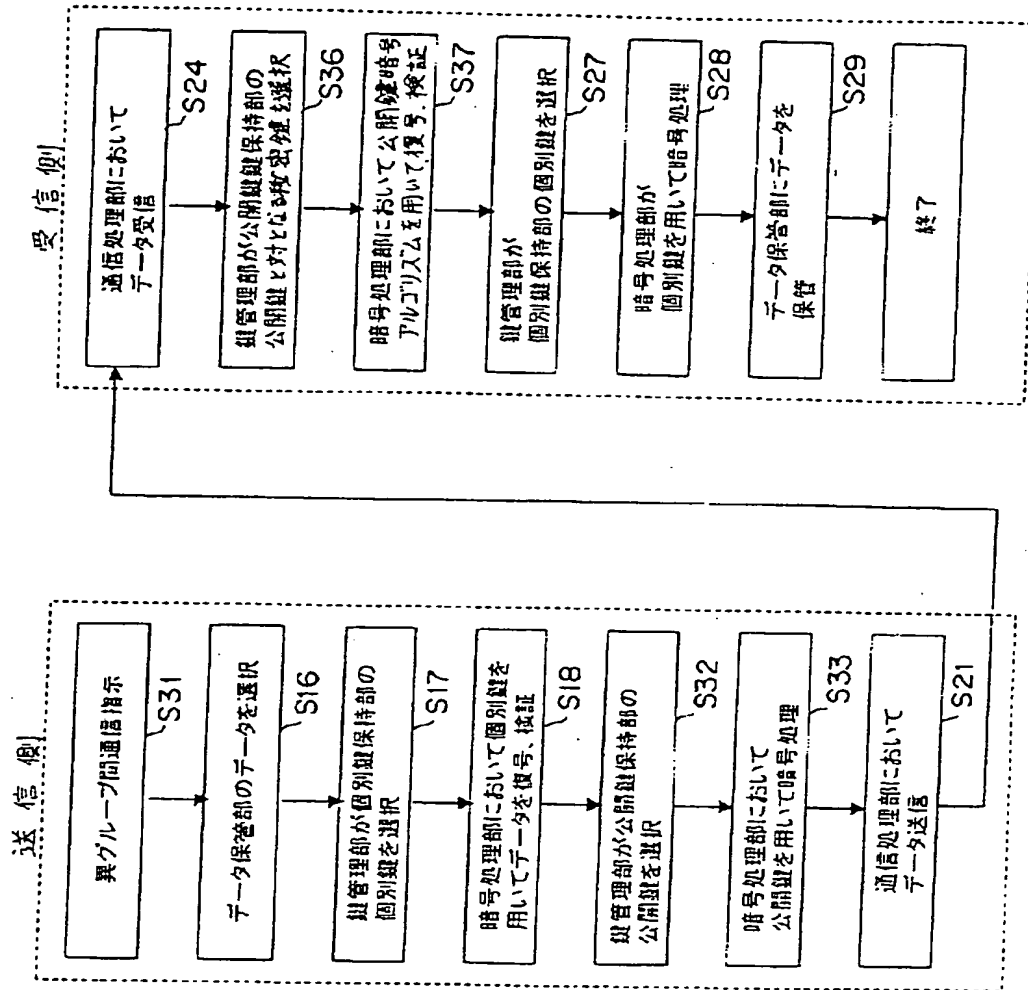
【図 4】

同一グループに属する電子データ保管装置との間での
データ送受信処理のフローチャート



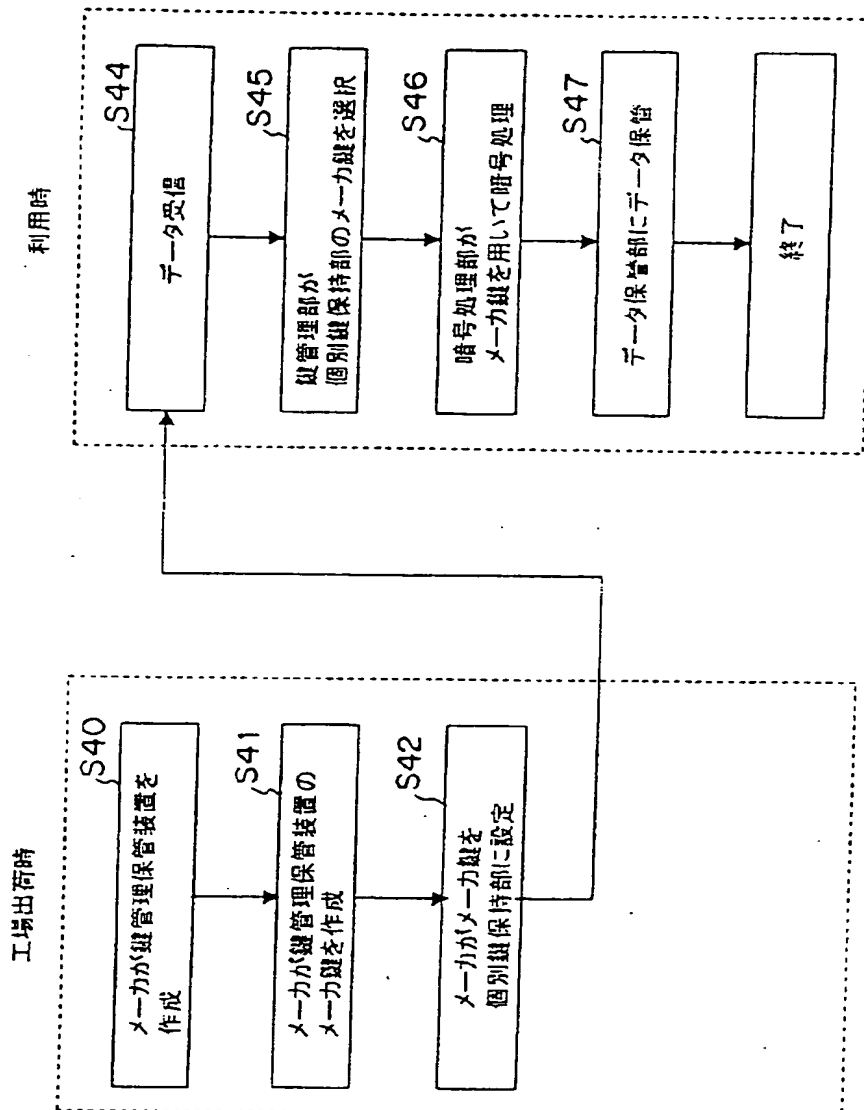
〔図 5〕

異なるグループに属する電子データ保管装置との
間でのデータ送受信処理のフローチャート



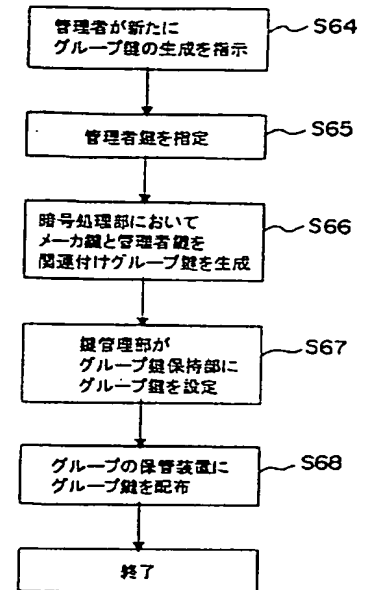
【図 6】

個別キーがあらかじめ割当てられている場合の
電子データ保管処理のフローチャート



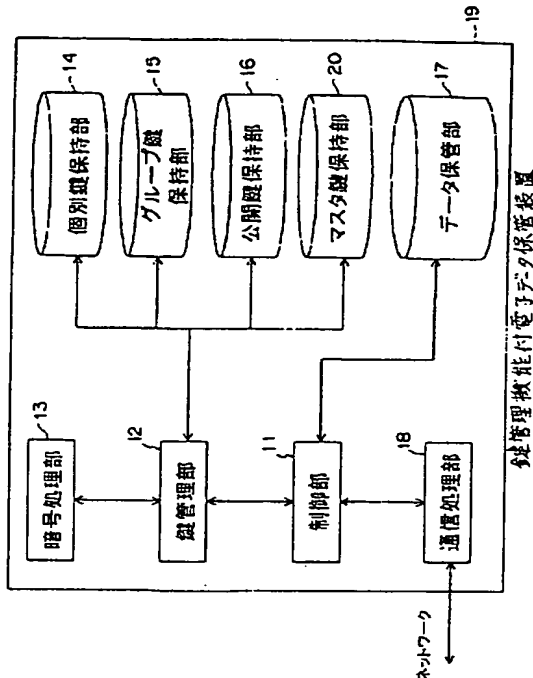
【図 10】

2つの鍵を関連づけてグループ鍵を
生成する処理のフローチャート



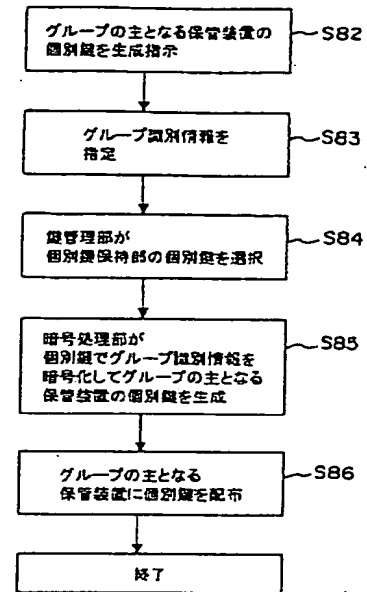
【図 11】

第2の実施形態における
電子データ保管装置の構成を示すブロック図



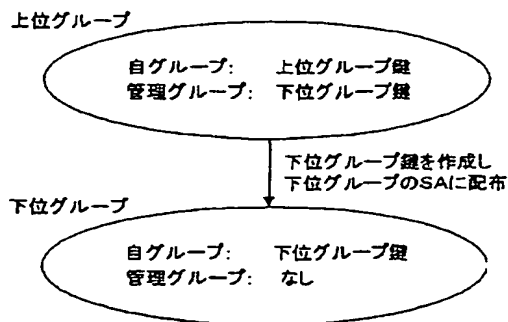
【図 14】

グループ管理保管装置による
グループマスタの個別鍵生成処理のフローチャート



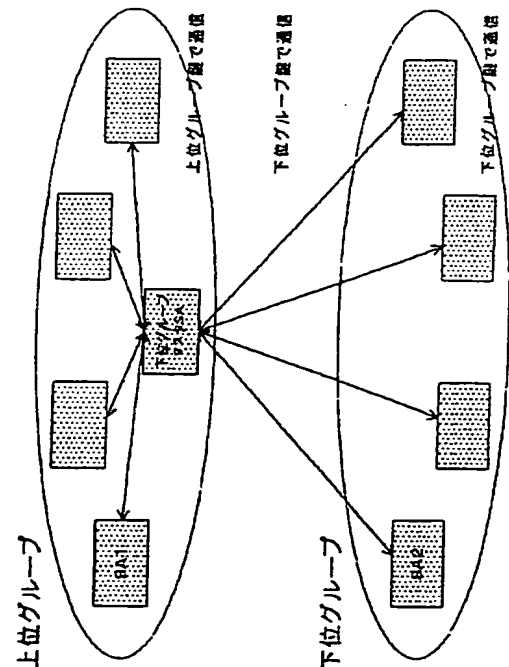
【図 15】

グループの階層化を説明する図



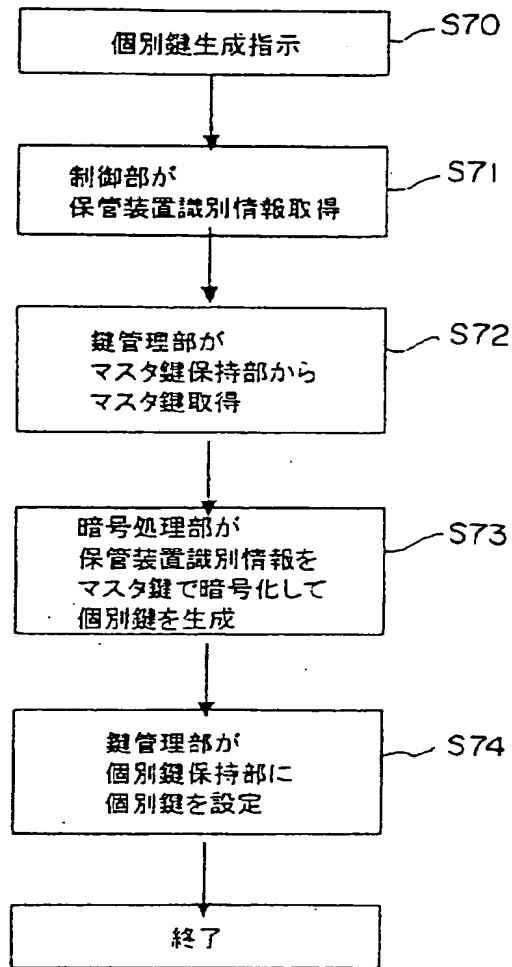
【図 16】

上位グループと下位グループの電子データ
保管装置相互間での通信を説明する図



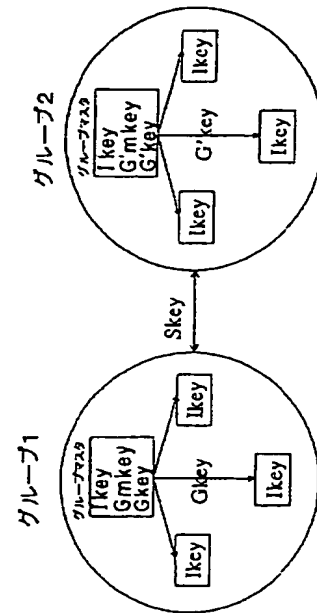
【図12】

第2の実施形態における
マスタ鍵を用いた個別鍵生成処理のフローチャート



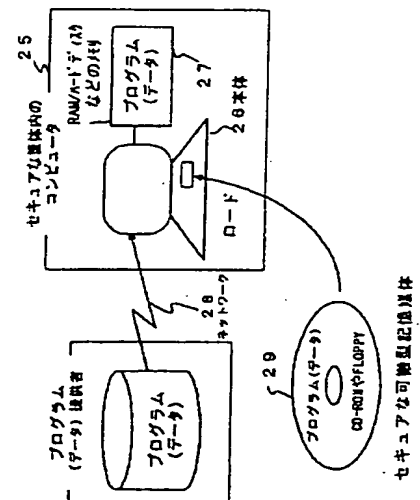
【図23】

グループ鍵の生成とその配布を説明する図



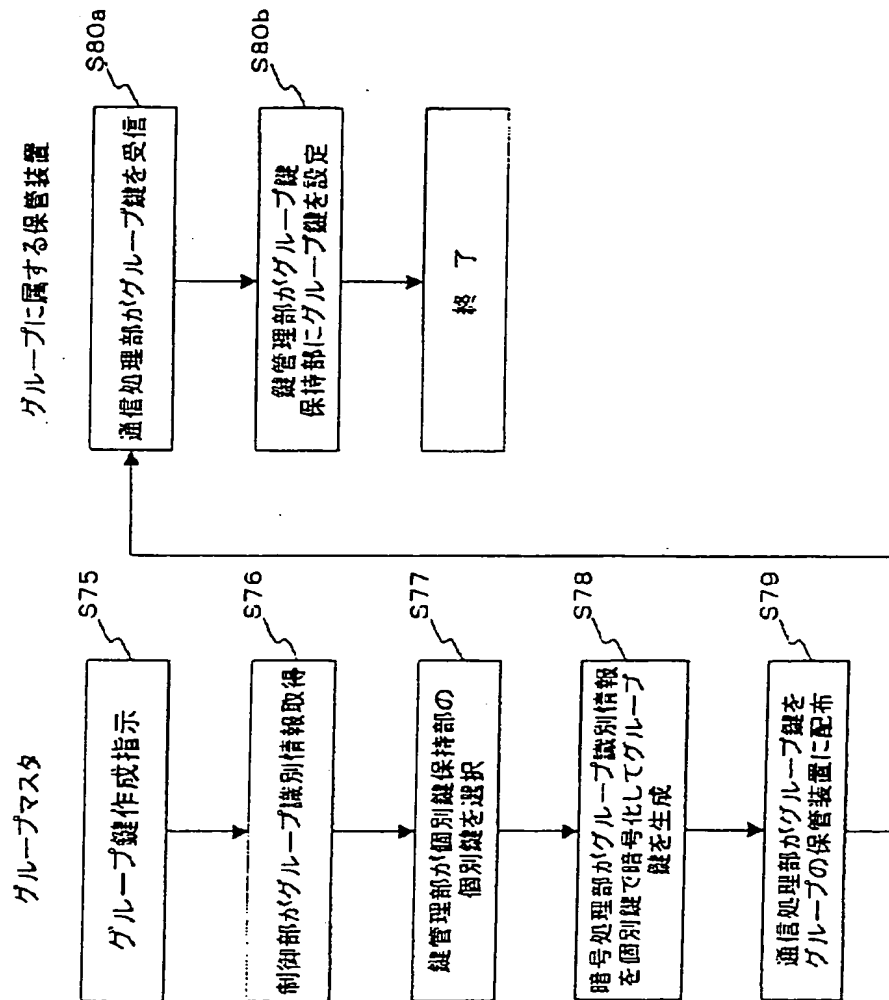
【図25】

本発明の電子データ保管装置を実現するための
プログラムのコンピュータへのローディングを説明する図



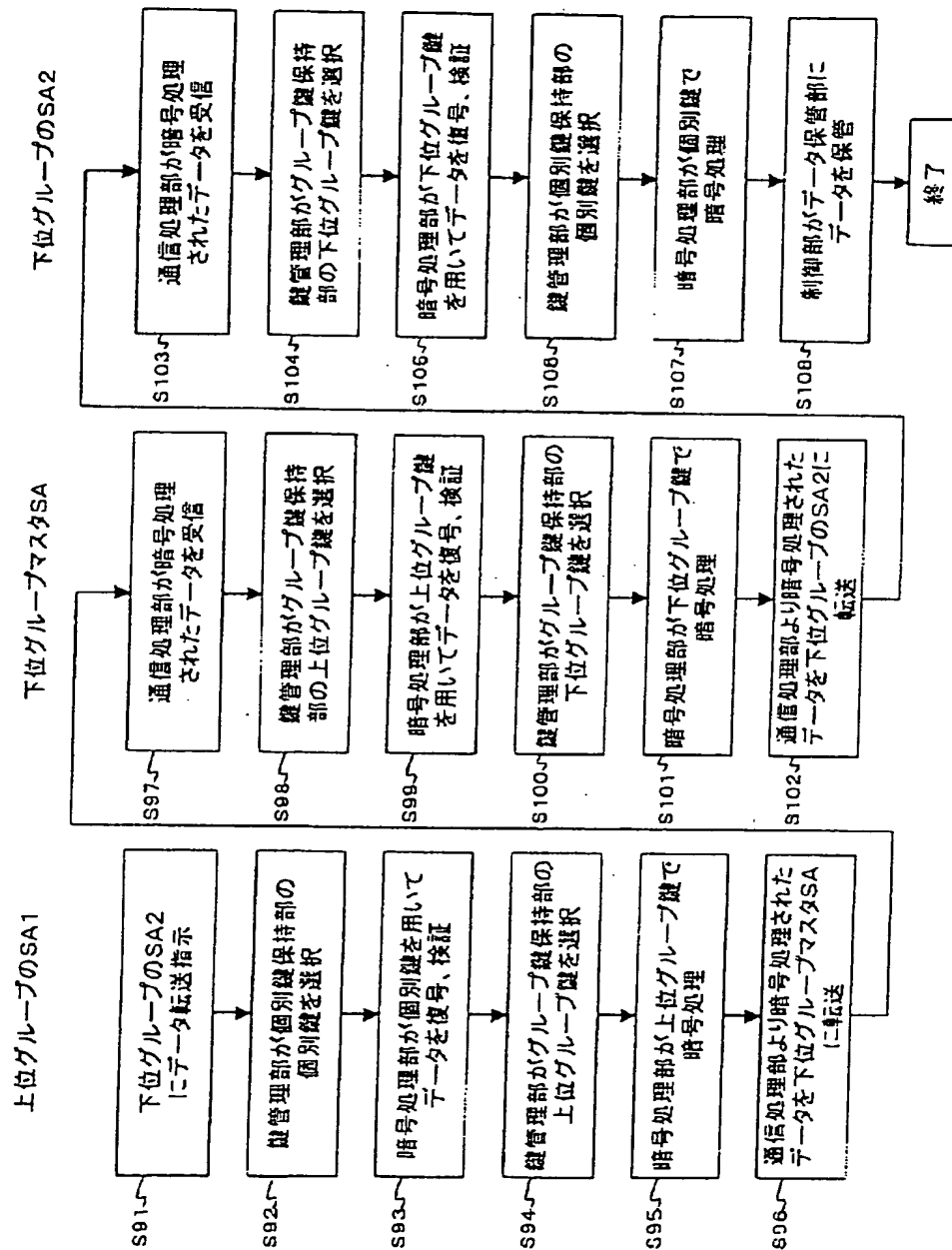
【図 13】

第 2 の実施形態における
グループ鍵生成処理のフローチャート



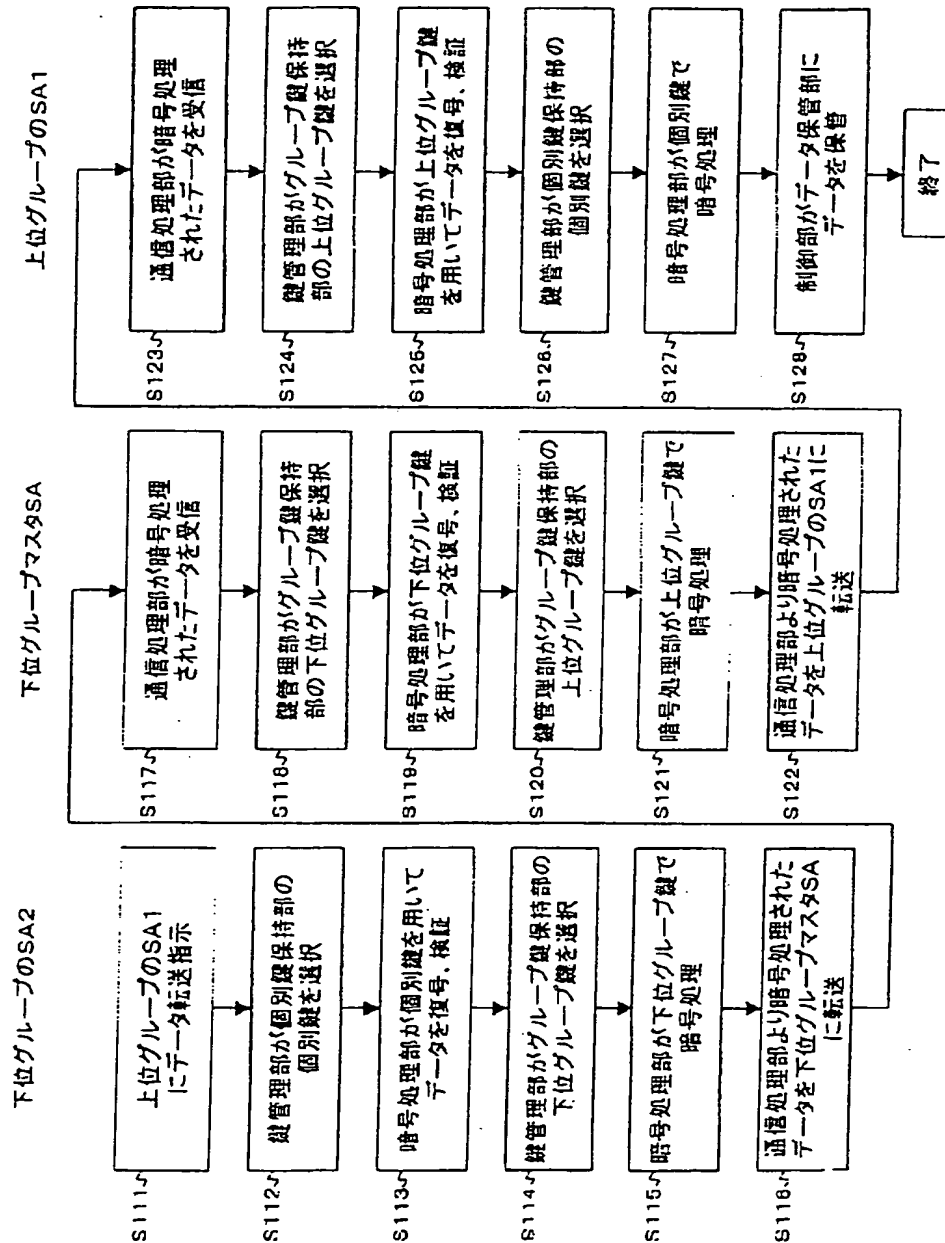
【図17】

上位グループの保管装置から
下位グループの保管装置へのデータ送信処理のフローチャート



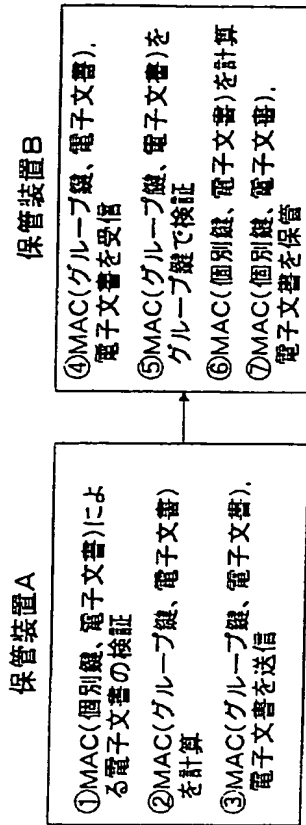
【図18】

下位グループの保管装置から
上位グループの保管装置へのデータ送信処理のフローチャート



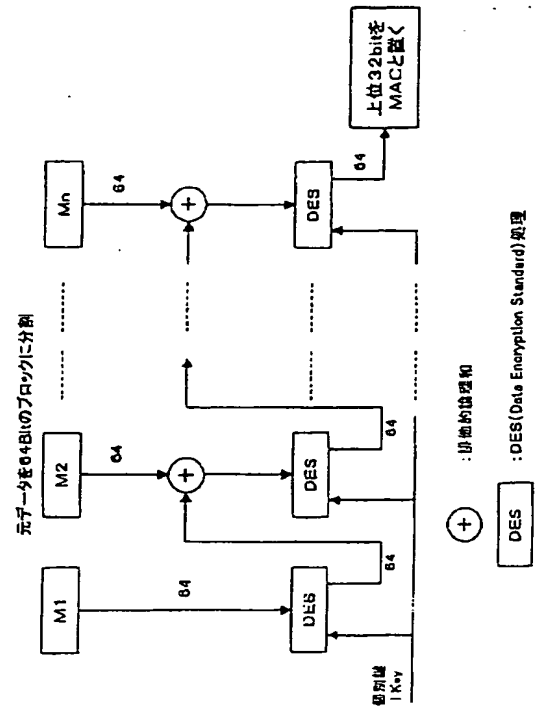
【図20】

同一グループに属する2つの
保管装置間のデータ送受信を説明する図



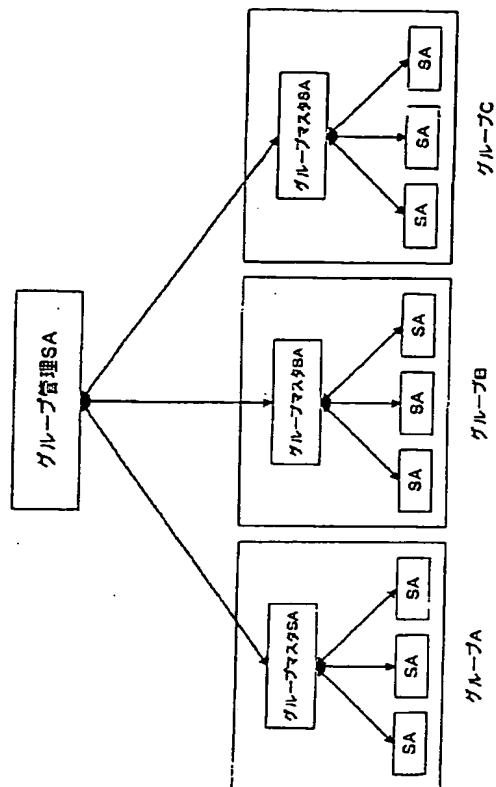
【図21】

改竄検出情報
MACの計算方法を説明する図



【図 24】

それぞれ複数のSAによって構成されるグループが複数存在する場合の、グループ管理SAによる全体管理方式の説明図



フロントページの続き

- (72)発明者 岩瀬 詔子
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
- (72)発明者 野田 敏達
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
- (72)発明者 小野 越夫
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5B017 AA08 BA05 BA07 BB02 BB03
CA07 CA08 CA09 CA14 CA16
5J104 AA01 AA16 AA34 EA04 EA16
JA03 NA02 PA14
9A001 BB02 BB03 BB04 CC02 DD09
DD10 EE03 HH33 JJ07 JJ13
JJ16 JZ03 LL03